AO 106 (Rev. 04/10) Application for a Search Warrant

UNITED STATES DISTRICT COURT

for the

Northern District of Texas

In the Matter of the Search of
(Briefly describe the property to be searched or identify the person by name and address)
THE PREMISES LOCATED AT 7202 S. WESTMORELAND ROAD, APT. 1240, DALLAS, TEXAS 75237

Case No. 4:22-MJ-432

[FILED UNDER SEAL]

APPLICATION FOR AN ANTICIPATORY SEARCH WARRANT

I, a federal law enforcement officer or an attorney for the government, request a search warrant and state under penalty of perjury that I have reason to believe that on the following person or property *(identify the person or describe the property to be searched and give its location)*:
See Attachment A.

located in the Northern District of Texas, there is now concealed *(identify the person or describe the property to be seized)*:
See Attachment B.

The basis for the search under Fed. R. Crim. P. 41(c) is *(check one or more)*:

- ☑ evidence of a crime;
- ☑ contraband, fruits of crime, or other items illegally possessed;
- ☑ property designed for use, intended for use, or used in committing a crime;
- ☐ a person to be arrested or a person who is unlawfully restrained.

The search is related to a violation of:

Code Section	*Offense Description*
26 U.S.C. § 5861(d)	Receipt or Possession of an Unregistered Firearm

The application is based on these facts:
See attached affidavit of ATF Special Agent Ross R. Walker.

- ☑ Continued on the attached sheet.
- ☐ Delayed notice of _____ days (give exact ending date if more than 30 days: _____) is requested under 18 U.S.C. § 3103a, the basis of which is set forth on the attached sheet.

Ross R. Walker
Applicant's signature

Special Agent Ross R. Walker, ATF
Printed name and title

Sworn to me over the telephone or by other electronic means and signed by me pursuant to Fed.R.Crim.P.4.1.

Date: June 10, 2022 at 3:21 p.m.

J. Cureton
United States Magistrate Judge
Judge's signature

City and state: Fort Worth, Texas

Jeffrey L Cureton, United State Magistrate Judge
Printed name and title

AFFIDAVIT IN SUPPORT OF APPLICATION FOR SEARCH WARRANT

I, Ross Walker, being duly sworn, depose and state that:

INTRODUCTION AND AGENT BACKGROUND

1. I am a Special Agent (SA) with the United States Department of Justice, Bureau of Alcohol, Tobacco, Firearms and Explosives (ATF), and have been so employed since November of 2016. My federal law enforcement training included completing the Criminal Investigator Training Program at the Federal Law Enforcement Training Center (FLETC) in Glynco, GA, and the Special Agent Basic Training Program at the ATF National Academy. At the Federal Law Enforcement Training Center, I received training in federal law and procedure, physical tactics and defense, behavioral science, counterterrorism operations, and continuing case investigations and techniques. I have been involved in numerous investigations involving firearms and narcotics violations during my time as a Special Agent in the Dallas Field Division. Prior to my appointment as a Special Agent with ATF, I was an Intelligence Research Specialist with ATF for 3 years where I assisted in the investigation of crimes under ATF's purview. Prior to my employment with ATF, I served 20 years with the U.S. Navy, both combined and as a reservist as an Intelligence Officer with both Joint Special Operations Command and Naval Special Warfare.

2. I am currently assigned to the ATF Dallas Field Division, Dallas VII Field Office; and as result of my training and experience as an ATF Agent, I am familiar with federal firearm and ammunition laws. I am qualified in investigating crimes involving advertisement, sale, and distribution of firearms subject to the provisions of the National Firearms Act ("NFA") and investigations involving interstate firearms and ammunition trafficking.

3. Pursuant to 18 U.S.C. § 3051, I am empowered to enforce criminal laws of the United States. As a result of my training and experience, I am familiar with federal laws including provisions of the National Firearms Act ("NFA"), including, but not limited to violations of 26 U.S.C. §§ 5841 and 5861(d), which state that it shall be unlawful for any person to possess, sell, or distribute firearms subject to the provisions of the NFA without having paid the special (occupational) tax required by 26 U.S.C. § 5801 for the business or having registered as required by 26 U.S.C. § 5802 and 18 U.S.C. § 923(a), which state that anyone engaging in the business of firearms sales must be licensed.

4. This affidavit is made in support of an application for a warrant to search the premises described in Attachment A and located at **7202 S. Westmoreland Road, Apt. #1240, Dallas, Texas 75237 ("PREMISES")**, which is in the Dallas Division of the Northern District of Texas, for the items described in Attachment B.

5. The information contained in this affidavit is based upon my personal knowledge, consultation with other ATF agents, consultation with other law enforcement officers, a review of documents and reports, interviews, and information provided to me by other law enforcement officers and agents of the United States. The information in this affidavit is not a complete statement of all the facts related to this case.

INVESTIGATION AND PROBABLE CAUSE

6. The ATF is currently conducting a criminal investigation of JEREMIAH ASHLEY regarding violations of 26 U.S.C. § 5861(d), which prohibits receiving or possessing a firearm that is not registered to him in the National Firearms Registration and Transfer Record (NFRTR).

7. ATF Special Agents currently assigned to ATF Dallas Group VII (Dallas Violent Crime Group), in conjunction with Garland Police Department (GPD), obtained information about a social media account advertising and selling Glock switches, sears, and firearms in the Dallas–Fort Worth area by Instagram account "2one4jay_."

8. On May 24, 2022, I received information from Investigator Logan Riley with GPD regarding the advertisement of Glock conversion switches (or "Glock switches") on Instagram, a social media and messaging application, and specifically account 2one4jay_. A Glock switch is a device designed and intended for use in converting a semiautomatic Glock pistol into an automatic machinegun. Because a Glock switch is a "machinegun" as defined by 26 U.S.C. § 5845(b), it may be possessed by only properly licensed Federal Firearms Licensees who have paid the appropriate Special Occupational Tax (SOT) required under the NFA and must be registered in the NFRTR.

9. The information I received from Investigator Riley indicated that Glock switches were being advertised for sale on Instagram under the username 2one4jay_. Instagram user 2one4jay_ posted a photograph of approximately sixteen (16) Glock switches and other various AR-style rifles as well as pistols with attached high-capacity magazines. The phrase "4 A POP" was overlayed on a picture of Glock switches. The same Instagram account showed videos of Glock pistols operating in automatic fashion utilizing a Glock switch.

10. Investigator Riley informed Special Agents Ross Walker and Michael Wasilewski from ATF about the advertising of Glock switches. It was agreed upon that a controlled purchase of the Glock switches would be attempted by Investigator Riley operating in an undercover capacity that same day, May 24, 2022.

11. Investigator Riley made contact with 2one4jay_ to arrange the purchase of three (3) Glock Switches. During the messaging conversation, 2one4jay_ stated that each Glock switch would cost $400, bringing the total of the three devices to $1,200. Investigator Riley agreed to the price and requested that the transaction take place at a RaceTrac gas station located at 4214 Forest Lane, Garland, Dallas County, Texas. 2one4jay_ agreed.

12. Investigator Riley arrived at the RaceTrac and informed 2one4jay_ that he was there. 2one4jay_ stated he was in a gray BMW. Investigator Riley parked his vehicle at the eastmost parking stall and waited. A few moments later, a gray BMW bearing Texas license plate PMV-0992 pulled behind Investigator Riley's vehicle and a black male got out of the driver seat. The black male's appearance was suspicious to Investigator Riley because he thought that 2one4jay_ was going to be a white Hispanic male due to his posts on Instagram. The black male got out of the driver seat, walked around to the front passenger side window, and took something through the slightly opened window from an occupant who was sitting there. The black male approached the driver side window of Investigator Riley's vehicle, and the two greeted each other. The black male reached out with an open hand containing three Glock switches. Investigator Riley handed the black male the required $1,200, which the black male took before placing the Glock switches in Investigator Riley's hand.

13. Investigator Riley asked the black male how the switch worked. The black male showed Investigator Riley how to assemble the switches and played a video on his phone of him (the black male) installing a Glock switch on a Glock pistol. Once the deal was done, the two separated and drove away from the RaceTrac.

14. Investigator Riley returned to a GPD police station, where he transferred possession of the Glock switches over to ATF SA Wasilewski. None of the Glock switches had serial numbers and, as a result, none of them could be registered in the NFRTR.

15. Investigator Riley found through Vigilant license plate recognition software that the gray BMW was last found to be in the parking garage at Palladium Redbird Apartments, 7202 S. Westmoreland Road, Dallas, Texas.

16. Separately, a screen shot of the undercover deal in which Investigator Riley purchased the Glock switches was sent to Texas Department of Public Safety (DPS) in an attempt to identify the black male. Texas DPS returned information identifying the black male as JEREMIAH DWYEN ASHLEY with a possible address of 7202 S. Westmoreland Road, Apt. #1240, Dallas, Texas 75237.

17. On June 8, 2022, ATF and GPD attempted another undercover purchase of Glock switches from 2one4jay_. Investigator Riley initiated communication, to which 2one4jay responded via messaging that the Glock switches would be delivered on Friday, June 10, 2022. 2one4jay_ sent a screen shot of UPS tracking information for a package to Investigator Riley.

18. ATF Special Agents reached out to UPS security personnel with that tracking information. UPS personnel explained that the package was one of three packages that are all part of the same shipment from a company in Taiwan and addressed to the **PREMISES**:

JERMINE ASHLEY
7202 S. Westmoreland Rd.
Apt. #1240
Dallas, TX 75237

Based on my review of law enforcement databases and reports, JERMINE ASHLEY is JEREMIAH ASHLEY's brother. The destination address for the three packages matches the address DPS associated with JEREMIAH ASHLEY and is consistent with where Vigilant license plate tracking software tracked the gray BMW involved in the controlled purchase. UPS personnel provided investigators with the following tracking numbers for the three packages: 1Z2V83E60409097232, 1Z2V83E60415807640, and 1Z2V83E60406505251.

19. A search of the NFRTR database for any firearms registered to JEREMIAH ASHLEY or JERMINE ASHLEY, each with the date of birth April 25, 2000, yielded no results. This search confirmed that neither JEREMIAH ASHLEY nor JERMINE ASHLEY have any NFA firearms registered to them.

20. On June 10, 2022, U.S. Magistrate Judge Jeffrey L. Cureton signed a warrant authorizing the seizure and search of the three UPS packages. Investigators searched the packages at a UPS distribution center in Arlington, Texas that same day.

21. The packages contained clear baggies with disassembled Glock switches and screws inside them. Based on my training and experience, I suspect that the sender surrounded the Glock switches in small screws to obscure the baggies' contents. Investigators limited the search to confirming that the packages contained Glock switches. But based on what I observed,

I estimate that there are approximately thirty (30) Glock switches inside the three packages.

CONTROLLED DELIVERY

22. Investigators worked with UPS personnel to intercept the three packages before delivery. The packages were on a sure course for delivery to the **PREMISES** until investigators intercepted them in Arlington, Texas.

23. As part of the investigation, I and other law enforcement offers intend to complete the delivery of the three packages to the **PREMISES**. The delivery is meant to confirm that JEREMIAH ASHLEY and/or JERMINE ASHLEY live(s) at the **PREMISES** and that the Glock switches are intended for one or both of them.

24. Using a controlled delivery technique, investigators plan to deliver the packages to an occupant of the **PREMISES**. After waiting a reasonable time to give the **PREMISES'** occupants an opportunity to open the packages and review their contents, investigators will recover the packages to prevent the occupants from using the contents to perpetrate any crimes. Investigators will execute this warrant to search the **PREMISES** only if an occupant of the **PREMISES** takes possession of the packages and then takes them inside the **PREMISES**.

COMPUTERS, ELECTRONIC STORAGE, AND FORENSIC ANALYSIS

25. As described above and in Attachment B, this application seeks permission to search for records that might be found on the **PREMISES**, in whatever form they are found. One form in which the records might be found is data stored on an electronic device, computer's hard drive, or other storage media. Thus, the warrant applied for would authorize the seizure of electronic storage media or, potentially, the copying of electronically stored information, all under Rule 41(e)(2)(B).

26. *Probable cause.* I submit that if a computer or storage medium is found on the **PREMISES**, there is probable cause to believe those records will be stored on that computer or storage medium, for at least the following reasons:

a. This investigation began after law enforcement discovered the advertisement of Glock switches on Instagram, a social media and messaging application, from user 2one4jay_. Law enforcement then investigated by having Investigator Riley communicate via Instagram in an undercover capacity with the individual who was advertising the Glock switches.

b. Several of the messages on Instagram were messages and pictures advertising the sale of Glock switches, pistols with high capacity magazines, and AR-style rifles.

c. During the controlled purchase, the black male later identified as JEREMIAH ASHLEY showed Investigator Riley a video of ASHLEY installing a Glock switch onto a Glock pistol on his cellular phone that was not previously shared via social media

d. Based on my training and experience, I know social media accounts such as Instagram are often accessed by individuals through cellular telephone devices, tablets, iPads, home computers, laptop computers and other portable electronic devices.

e. Based on my knowledge, training, and experience, I know that computer files or remnants of such files can be recovered months or even years after they have been downloaded onto a storage medium, deleted, or viewed via the Internet. Electronic files downloaded to a storage medium can be stored for years at little or no cost. Even when files have been deleted, they can be recovered months or years later using forensic tools. This is so because when a person "deletes" a file on a computer, the data contained in the file does not actually disappear; rather, that data remains on the storage medium until it is overwritten by new data.

f. Therefore, deleted files, or remnants of deleted files, may reside in free space or slack space—that is, in space on the storage medium that is not currently being used by an active file—for long periods of time before they are overwritten. In addition, a computer's operating system may also keep a record of deleted data in a "swap" or "recovery" file.

g. Wholly apart from user-generated files, computer storage media—in particular, computers' internal hard drives—contain electronic evidence of how a computer has been used, what it has been used for, and who has used it. To give a few examples, this forensic evidence can take the form of operating system configurations, artifacts from operating system or application operation, file system data structures, and virtual memory "swap" or paging files.

Computer users typically do not erase or delete this evidence, because special software is typically required for that task. However, it is technically possible to delete this information.

h. Similarly, files that have been viewed via the Internet are sometimes automatically downloaded into a temporary Internet directory or "cache."

27. *Forensic evidence.* As further described in Attachment B, this application seeks permission to locate not only computer files that might serve as direct evidence of the crimes described on the warrant, but also for forensic electronic evidence that establishes how computers were used, the purpose of their use, who used them, and when. There is probable cause to believe that this forensic electronic evidence will be on any storage medium in the **PREMISES** because:

a. Data on the storage medium can provide evidence of a file that was once on the storage medium but has since been deleted or edited, or of a deleted portion of a file (such as a paragraph that has been deleted from a word processing file). Virtual memory paging systems can leave traces of information on the storage medium that show what tasks and processes were recently active. Web browsers, e-mail programs, and chat programs store configuration information on the storage medium that can reveal information such as online nicknames and passwords. Operating systems can record additional information, such as the attachment of peripherals, the attachment of USB flash storage devices or other external storage media, and the times the computer was in use. Computer file systems can record information about the dates files were created and the

sequence in which they were created, although this information can later be falsified.

b. As explained herein, information stored within a computer and other electronic storage media may provide crucial evidence of the "who, what, why, when, where, and how" of the criminal conduct under investigation, thus enabling the United States to establish and prove each element or alternatively, to exclude the innocent from further suspicion. In my training and experience, information stored within a computer or storage media (e.g., registry information, communications, images and movies, transactional information, records of session times and durations, internet history, and anti-virus, spyware, and malware detection programs) can indicate who has used or controlled the computer or storage media. This "user attribution" evidence is analogous to the search for "indicia of occupancy" while executing a search warrant at a residence. The existence or absence of anti-virus, spyware, and malware detection programs may indicate whether the computer was remotely accessed, thus inculpating or exculpating the computer owner. Further, computer and storage media activity can indicate how and when the computer or storage media was accessed or used. For example, as described herein, computers typically contain information that log: computer user account session times and durations, computer activity associated with user accounts, electronic storage media that connected with the computer, and the IP addresses through which the computer accessed networks and the internet. Such information allows investigators to understand the chronological context of computer or electronic storage media access, use, and

events relating to the crime under investigation. Additionally, some information stored within a computer or electronic storage media may provide crucial evidence relating to the physical location of other evidence and the suspect. For example, images stored on a computer may both show a particular location and have geolocation information incorporated into its file data. Such file data typically also contains information indicating when the file or image was created. The existence of such image files, along with external device connection logs, may also indicate the presence of additional electronic storage media (e.g., a digital camera or cellular phone with an incorporated camera). The geographic and timeline information described herein may either inculpate or exculpate the computer user. Last, information stored within a computer may provide relevant insight into the computer user's state of mind as it relates to the offense under investigation. For example, information within the computer may indicate the owner's motive and intent to commit a crime (e.g., internet searches indicating criminal planning), or consciousness of guilt (e.g., running a "wiping" program to destroy evidence on the computer or password protecting/encrypting such evidence in an effort to conceal it from law enforcement).

c. A person with appropriate familiarity with how a computer works can, after examining this forensic evidence in its proper context, draw conclusions about how computers were used, the purpose of their use, who used them, and when.

d. The process of identifying the exact files, blocks, registry entries, logs, or other forms of forensic evidence on a storage medium that are necessary to draw an accurate conclusion is a dynamic process. While it is possible to specify in

advance the records to be sought, computer evidence is not always data that can be merely reviewed by a review team and passed along to investigators. Whether data stored on a computer is evidence may depend on other information stored on the computer and the application of knowledge about how a computer behaves. Therefore, contextual information necessary to understand other evidence also falls within the scope of the warrant.

e. Further, in finding evidence of how a computer was used, the purpose of its use, who used it, and when, sometimes it is necessary to establish that a particular thing is not present on a storage medium. For example, the presence or absence of counter-forensic programs or anti-virus programs (and associated data) may be relevant to establishing the user's intent.

28. *Necessity of seizing or copying entire computers or storage media.* In most cases, a thorough search of a premises for information that might be stored on storage media often requires the seizure of the physical storage media and later off-site review consistent with the warrant. In lieu of removing storage media from the premises, it is sometimes possible to make an image copy of storage media. Generally speaking, imaging is the taking of a complete electronic picture of the computer's data, including all hidden sectors and deleted files. Either seizure or imaging is often necessary to ensure the accuracy and completeness of data recorded on the storage media, and to prevent the loss of the data either from accidental or intentional destruction. This is true because of the following:

a. The time required for an examination. As noted above, not all evidence takes the form of documents and files that can be easily viewed on site. Analyzing evidence of how a computer has been used, what it has been used for, and who

has used it requires considerable time, and taking that much time on premises could be unreasonable. As explained above, because the warrant calls for forensic electronic evidence, it is exceedingly likely that it will be necessary to thoroughly examine storage media to obtain evidence. Storage media can store a large volume of information. Reviewing that information for things described in the warrant can take weeks or months, depending on the volume of data stored, and would be impractical and invasive to attempt on-site.

b. Technical requirements. Computers can be configured in several different ways, featuring a variety of different operating systems, application software, and configurations. Therefore, searching them sometimes requires tools or knowledge that might not be present on the search site. The vast array of computer hardware and software available makes it difficult to know before a search what tools or knowledge will be required to analyze the system and its data on the **PREMISES**. However, taking the storage media off-site and reviewing it in a controlled environment will allow its examination with the proper tools and knowledge.

c. Variety of forms of electronic media. Records sought under this warrant could be stored in a variety of storage media formats that may require off-site reviewing with specialized forensic tools.

29. *Nature of examination.* Based on the foregoing, and consistent with Rule 41(e)(2)(B), the warrant I am applying for would permit seizing, imaging, or otherwise copying storage media that reasonably appear to contain some or all of the evidence described in the warrant, and would authorize a later review of the media or information consistent with the warrant.

The later review may require techniques, including but not limited to computer-assisted scans of the entire medium, that might expose many parts of a hard drive to human inspection in order to determine whether it is evidence described by the warrant.

CONCLUSION

30. I submit that this affidavit supports probable cause for a warrant to search the **PREMISES** described in Attachment A and seize the items described in Attachment B.

Ross R. Walker
Special Agent
Bureau of Alcohol, Tobacco,
Firearms and Explosives

Sworn to me, over the telephone or other electronic means, and signed by me pursuant to Fed. R. Crim. P. 4.1 on this 10th day of June 2022, at 3:21 p.m. in Fort Worth, Texas.

JEFFREY L. CURETON
UNITED STATES MAGISTRATE JUDGE

ATTACHMENT A

Description of the Property to Be Searched

The apartment unit located at 7202 S. Westmoreland Road, Apt. #1240, Dallas, Texas 75237. The apartment unit is in the Dallas Division of the Northern District of Texas.

ATTACHMENT B

Items to Be Seized

1. Items that constitute fruits, evidence, information, contraband, or instrumentalities relating to violations of 26 U.S.C. §§ 5841, 5861(d) and 18 U.S.C. § 923(a). The items to be seized include:

a. firearms (including conversion devices such as Glock switches)

b. ammunition;

c. firearm cases and boxes;

d. firearm accessories (including, but not limited to, holsters and magazines);

e. firearms parts (whole or partial, dissembled or assembled);

f. bill of sale records (whether real or fictitious);

g. sales receipts and other financial records;

h. U.S. currency;

i. indicia of occupancy;

j. documentation (whether real or fictitious) that would facilitate the procurement and/or possession of firearms;

k. records of communications that advertise or facilitate the procurement and/or sale of firearms;

l. and photographs.

2. For any computer or storage medium whose seizure is otherwise authorized by this warrant, and any computer or storage medium that contains or in which is stored records or information that is otherwise called for by this warrant (hereinafter, "COMPUTER"):

j. documentation and manuals that may be necessary to access the COMPUTER or to conduct a forensic examination of the COMPUTER;

k. records of or information about Internet Protocol addresses used by the COMPUTER;

l. records of or information about the COMPUTER's Internet activity, including firewall logs, caches, browser history and cookies, "bookmarked" or "favorite" web pages, search terms that the user entered into any Internet search engine, and records of user-typed web addresses;

m. contextual information necessary to understand the evidence described in this attachment.

As used above, the terms "records" and "information" includes all forms of creation or storage, including any form of computer or electronic storage (such as hard disks or other media that can store data); any handmade form (such as writing); any mechanical form (such as printing or typing); and any photographic form (such as microfilm, microfiche, prints, slides, negatives, videotapes, motion pictures, or photocopies).

The term "computer" includes all types of electronic, magnetic, optical, electrochemical, or other high speed data processing devices performing logical, arithmetic, or storage functions, including desktop computers, notebook computers, mobile phones, tablets, server computers, and network hardware.

The term "storage medium" includes any physical object upon which computer data can be recorded. Examples include hard disks, RAM, floppy disks, flash memory, CD-ROMs, and other magnetic or optical media.

Attachment B